Memorandum

To: Business Transportation and Housing Agency   **Date:**   February 22, 2002
Department of Information Technology
Teale Data Center Customers
Information Security Officers

From: **Stephen P. Teale Data Center**

Subject: **CERT Advisory CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)**

The Teale Data Center has conducted a preliminary assessment of its status related to the recent CERT Advisory on Simple Network Management Protocol (SNMP) Vulnerabilities (CA-2002-03), and is taking a number of steps to protect its systems from the noted vulnerabilities.

SNMP is a widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, server, etc.), to the workstation console used to oversee the network. The agents return information that defines what is obtainable from the device and what can be controlled (turned off, on, etc.). Originating in the UNIX community, SNMP has become widely used on all major platforms.
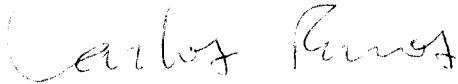
Although these vulnerabilities have been published, there have been no announced exploits at this time. We have completed the following actions:

- Blocked all incoming SNMP from the Internet into CSGNet,
- Blocked all incoming SNMP from external sources into Teale's internal network except where required for business, and
- Disabled SNMP on those devices where it is not necessary.

The following actions are in progress:

- Evaluating specifically which of our systems are vulnerable,
- Developing a project plan to apply vendor fixes for this problem as soon as they are released,
- Evaluating measures to heighten our resistance to any future SNMP vulnerabilities, and
- Monitoring vendor websites for latest developments.

Additional notification will be provided as we complete the action items or obtain additional information. If you have any questions regarding this communication, you may contact Sharon Smith, Teale's Information Security Officer, at (916) 464-4508 (CALNET 433-4508).

CARLOS RAMOS
Director